

(19) 대한민국특허청(KR)  
 (12) 공개특허공보(A)

(51) Int. Cl. <sup>7</sup> G06F 1/00	(11) 공개번호 특2003-0029068 (43) 공개일자 2003년04월11일
(21) 출원번호 10-2003-0009991	
(22) 출원일자 2003년02월18일	
(71) 출원인 (주)비트와이어	
	경기도 고양시 덕양구 행주내동 186-1
(72) 발명자 신동엽	
	서울특별시 송파구 가락본동 781T 벤처타워 동관 414호

심사청구 : 있음

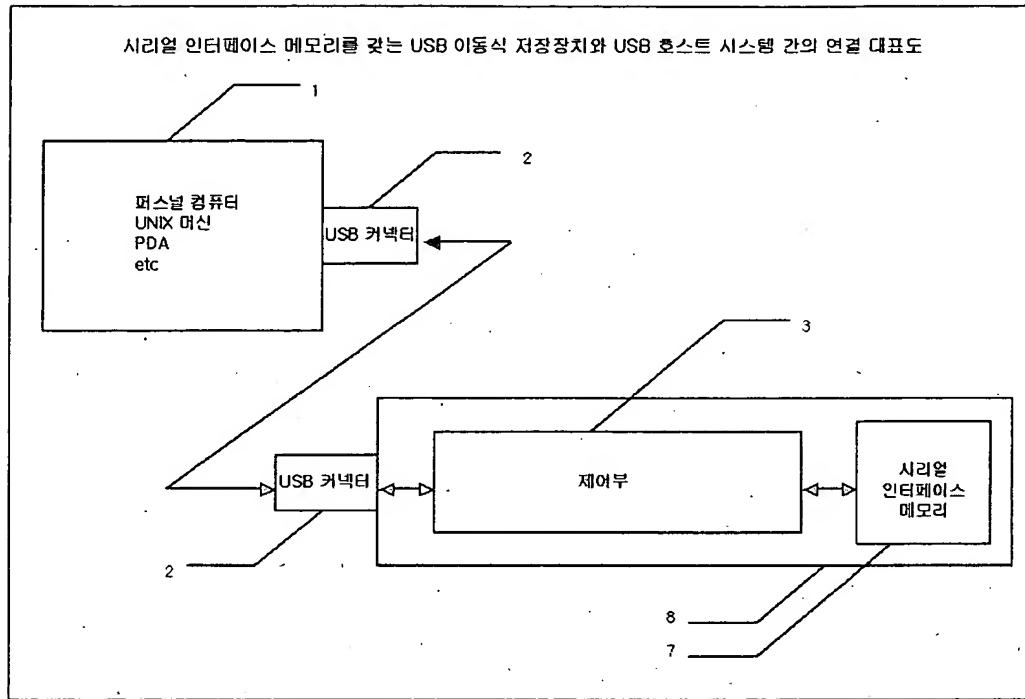
(54) 시리얼 인터페이스 메모리를 이용한 FAT(File Allocation Table) 파일 시스템방식의 보안 인증  
용 USB 이동식 저장 장치

요약

본 발명은 소용량의 시리얼 인터페이스 메모리를 1개 혹은 2개 이상 사용하여 대용량 파일 시스템인 FAT(File Allocation Table) 파일 시스템을 적용하여 보안 인증용 USB 이동식 저장 장치 드라이브로서, 종래에는 대용량 플래시 메모리를 사용하였으나 소용량의 시리얼 메모리에 FAT 파일 시스템을 적용하지 못해 일반적인 컴퓨터 시스템에서 보안 토큰용 장치와 각 보안 프로그램간에 호환성의 문제가 있었으나 본 발명으로 상기 문제를 해소한다. 상세하게는 보안 토큰용 데이터 및 일반 파일 데이터가 저장되는 수십 Kbyte 의 소용량 시리얼 인터페이스 메모리와, 상기 메모리에 상기 보안 토큰용 데이터 및 일반 파일 데이터의 송수신을 제어하며, 상기 일반 파일 데이터와 보안 토큰용 데이터를 상기 메모리에 대용량 파일 시스템인 FAT의 형태로 기록, 변경, 삭제를 수행하고, 상기 보안 토큰용 데이터에 대해서는 서명, 검증, 암호를 생성, 기록, 변경, 삭제를 수행하는 시리얼 인터페이스 메모리를 갖는 USB 이동식 저장 장치이다.

또한 일반적인 컴퓨터에서 사용하는 파일 시스템인 FAT를 이용하여 이동식 저장 장치 드라이브 형태로 사용할 수 있기 때문에 종래의 컴퓨터 시스템과 보안 프로그램에 따른 호환성 및 불규칙한 데이터 저장 형태를 해결할 수 있는 것을 특징으로 한다.

## 대표도



## 색인어

USB, 인증, 토큰, 암호, 이동식, FAT

## 영세서

## 도면의 간단한 설명

도 1은 시리얼 인터페이스 메모리를 이용한 USB 이동식 저장장치와 USB 호스트 시스템 간의 연결 상세도  
도 2는 시리얼 인터페이스 메모리를 이용한 USB 이동식 저장장치에 2개 이상의 시리얼 인터페이스 메모리 연결을 나타내는 상세도

도 3은 시리얼 인터페이스 메모리를 이용한 USB 이동식 저장장치에 2개 이상의 시리얼 인터페이스 제어부가 연결되고, 각각의 시리얼 인터페이스 제어부에 1개 혹은 2개 이상의 시리얼 인터페이스 메모리 연결을 나타내는 상세도

도 4는 시리얼 인터페이스 메모리를 이용한 USB 이동식 저장장치에 암호화 블록이 포함된 상세도

## 발명의 상세한 설명

## 발명의 목적

## 발명이 속하는 기술 및 그 분야의 종래기술

시리얼 인터페이스 메모리는 (a) 적은 용량을 갖는 메모리 반도체에 적은 비용으로 반도체를 포장(패키징)하기 위한 목적으로 (b) 큰 용량을 갖지만 최소한의 연결만으로 큰 용량의 데이터를 읽고 쓰기 위해서 만들어진 방식을 의미한다.

또한 시리얼 인터페이스 메모리에 있어서 가장 많이 사용되고 있는 대표적인 시리얼 인터페이스 방식은 필립스사에서 제안한 I<sup>2</sup>C이다. 여기서 I<sup>2</sup>C는 I<sup>2</sup>C와 같은 표현이며, 2개의 라인만으로 병렬로 연결된 많은 수의 메모리 혹은 다른 기능을 하는 디바이스를 제어 할 수 있다. 이 외에 3개 이상 9개 이하의 라인만으로도 연결이 가능한 시리얼 인터페이스는 각기 다른 알고리즘으로 존재한다.

여기서 시리얼 인터페이스 메모리는 부동게이트 트랜지스터로 구성되어 전기적 소거가 가능하고, 프로그래밍 가능하며 전원 공급 목적을 배제한 인터페이스를 위해 2개의 라인을 사용하는 시리얼 인터페이스 EEPROM을 포함하고, 비휘발성 메모리의 일종으로 DRAM의 gate oxide 또는 storage capacitor 재료를 강유전체로 대체하여 강유전체 재료의 특성인 높은 유전율이나 분극을 이용, DRAM이나 Non-volatile

memory 등 2가지로 사용할 수 있는 FeRAM을 포함한다. 여기서 FeRAM 역시 시리얼 인터페이스 방식으로 제어하는 것을 의미한다.

본 발명은 컴퓨터 시스템에서 소형 경량인 반도체 메모리를 이용한 병용 직렬 버스(universal serial bus : USB)를 이용하여 보조 기억 장치의 저장된 데이터를 관리하기 위한 구조 및 파일 시스템(FAT)의 방법에 관한 것이다.

최근 들어 플래시 메모리 중 NAND 형 플래시 반도체 메모리를 이용한 USB 이동식 저장장치가 기존의 하드·디스크 디바이스(hard disk device)나 플로피 디스크 디바이스(floppy disk device)등을 대체해 많이 사용되고 있다.

반도체 메모리를 이용한 USB 이동식 저장 장치는 플로피 디스크나 하드 디스크에 비해 휴대하기가 편리하고 충격으로부터 데이터가 손실될 위험성이 적다.

그러나, 앞서 설명한 바와 같이 반도체 메모리를 이용한 USB 이동식 저장 장치의 편리성에도 불구하고, 사용되고 있는 NAND형 플래시 메모리가 8Mbyte에서 최고 256Mbyte까지 고용량이고 고비용을 부담해야 한다. 따라서 몇 Kbyte에서 수십 Kbyte의 적은 용량만으로도 충분한 암호 및 전자서명 등이 필요한 시스템에서 사용 할 수 있고 일반 컴퓨터 시스템에서 특별한 소프트웨어나 하드웨어의 변경 없이 사용 가능한 새로운 USB 이동식 저장장치의 구조 및 파일 시스템(FAT)의 적용 방법이 요구된다. 여기서 특별한 소프트웨어나 하드웨어의 변경이 없다는 의미는 인증 파일 등과 같은 데이터 파일을 읽고 쓰는데 있어서 특정 소프트웨어나 하드웨어가 필요없음을 의미하며 보안 토큰을 위해서는 필요한 경우 특정 프로그램이나 특정 함수가 포함된 프로그램에 의해서 제어 가능함을 구분한다.

#### 발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 상기 상술한 요구 사항을 해결하기 위해 제안된 것으로, 컴퓨터 시스템의 종류 또는 컴퓨터 시스템에 장착된 특정 장치에 제한 받지 않고 수십 Kbyte 정도 만으로 필요한 보안 토큰용 데이터 등을 저장하는 이동식 저장장치가 가능한 방법을 제공하는데 있다.

#### 발명의 구성 및 작용

상기와 같은 목적을 달성하기 위해 본 발명에 따른 시리얼 인터페이스 메모리가 적어도 1개 이상 포함되어야 하며, 본 발명과 연결 위해 USB 호스트가 내장된 어신과 연결을 위한 USB 커넥터(2), 적어도 1개 이상의 시리얼 인터페이스 메모리(7, 10, 11, 12), 시리얼 인터페이스 메모리와 USB 신호를 처리하는 제어부(3)로 구성된다.

상기 구성과 같이 크게 세부분으로 구성이 이루어지며, 시리얼 인터페이스 메모리와 USB 신호를 처리하는 제어부를 좀더 구체적으로 상술한다. 상기 부분은 크게 다섯 부분으로 나눠지며, 상기 다섯부분은 각각 독립적으로 구성 될 수도 있다.

첫째 USB 호스트에서 전달하는 데이터를 마이컴 쪽에 전달하거나, USB 호스트에서 이동식 저장장치에서 요구하는 데이터를 마이컴으로부터 받아서 USB 호스트로 전달해주는 USB 컨트롤러(5)가 있으며,

두번째로 마이컴(4) 혹은 다른 제어부(6, 13)로부터 들어오는 데이터를 시리얼 인터페이스 메모리에 쓰거나, 요구하는 데이터를 읽어서 넘겨주는 역할을 하는 시리얼 인터페이스 제어부(9)가 있다. 시리얼 인터페이스 제어부는 도 2와 같이 1개가 존재 할 수 있고, 도3과 같이 2개 혹은 그 이상이 존재 할 수 있으며, 각각의 시리얼 인터페이스 제어부는 도 1과 같이 1개의 시리얼 인터페이스 메모리와 연결되어 구성될 수 있으며, 도 2, 도3과 같이 1개의 시리얼 인터페이스 제어부에서 각각 1개 혹은 2개 이상 시리얼 인터페이스 메모리를 구성하여 좀더 큰 용량을 갖는 저장 공간을 구성 할 수 있다.

세번째로 시리얼 인터페이스 메모리에 FAT(File Allocation Table) 자료 구조를 담당하는 코덱(6)이다. 상기 부분은 마이컴 제어부(4)에서 어플리케이션으로 구성될 수 있고, 하드웨어로 구성 할 수 있다. 또한 시리얼 메모리의 영역을 구분하여 서로 다른 영역에 각각의 FAT 파일 시스템을 구성하는 것 또한 가능하다.

네번째로 상기 세번째 항목에서 구성된 FAT 자료구조에 의거하여 저장된 파일 데이터를 가지고 보안 용도로 사용 가능하지만, 이것에 대한 2종 보안 목적으로 크립토 제어부(13)를 구성하여 보안 파일 자체의 데이터를 암호화하여 보안 파일을 읽고 쓰고, 삭제하거나, 각각의 시리얼 인터페이스 메모리를 갖는 USB 이동식 저장 장치 자체에 별도의 번호를 부여하여 사용자의 정보를 특수 프로그램을 통해서만 확인 가능하게 함으로써 높은 보안 수준을 유지하도록 구성 된다. 상기 부분 또한 상기 세번째 항과 마찬가지로 상기 제어부의 어플리케이션이나 하드웨어로 구성 한다.

마지막으로 상기4가지 항목을 종합적으로 관리하는 마이컴 제어부(4)가 있다. 상기 항목들간에 데이터 흐름을 관리 하도록 구성되어 있다. 데이터 흐름의 관리는 구체적으로 데이터가 전달되면 이를 통해 서

명, 검증, 암호, 복호, 해쉬, 랜덤값 생성 기록 변경 삭제를 모두 포함하는 관리를 의미한다.

### 발명의 효과

이상에서 설명한 바와 같은 본 발명은 기존의 제품군들과는 달리 시리얼 인터페이스 메모리 칩을 이용한 전자식 구동 방식에 의하여 구동되어 별다른 장치가 필요 없이 본 발명의 디바이스 드라이브를 설치 혹은 별도의 디바이스 드라이브의 설치 필요 없이 USB 디바이스를 PC 혹은 USB 호스트를 제공하는 모든 디바이스에 연결하여 시리얼 인터페이스 메모리를 갖는 USB 이동식 저장 장치로 사용이 가능하다.

또한, 생활 주변에서 사용하는 윈도우 환경 및 USB 호스트를 사용하고 USB 표준 인터페이스 방식을 제공하는 OS(Operating System)에서는 마치 하드디스크 드라이브와 같은 형태로 인식 및 사용한다.

그리고 장착된 시리얼 인터페이스 메모리 개수에 따라 고용량 외장 저장장치의 구현이 가능하다.

PC와 USB 호스트를 내장한 디바이스에 직접 연결이 되어 있어 휴대가 간편하고 시리얼 인터페이스 메모리를 사용하므로 매체 외관에 미치는 충격에 의한 수명 단축이나 소음이 없고 외부의 물리적 충격 및 자력에 의한 데이터 훼손의 확률이 매우 적으며 소형화가 가능하고 저비용으로 구현이 가능하다.

결론 지어 정리하면, 시리얼 인터페이스 메모리를 이용하여 여타 다른 메모리 반도체를 이용하는 것보다 소형화가 가능하며, 가격적인 면에서 상당히 저렴하게 저용량 이동식 저장장치 제작이 가능하고, 또한 FAT(File Allocation Table) 파일시스템이 적용 가능한 저용량 USB 이동식 저장장치로 인식 가능하게 하므로써 각각의 다른 방식으로 저장되어온 보안 토큰 방식을 일반화하여 서로 다른 부류의 토큰 방식을 통합할 수 있고, 동시에 또 다른 인식과정을 첨가 가능하게 하므로써 보안의 효과를 극대화 할 수 있다.

### (57) 청구의 범위

#### 청구항 1

USB로 정의된 버스에 접속하는 USB 이동식 저장 장치에 있어서 (a) 데이터를 저장하는 적어도 하나의 시리얼 인터페이스 메모리 모듈과 (b) USB 표준 규격에 맞게 데이터를 버스상에 입/출력하는 최종단이 USB 커넥터로 이루어지고, (c) USB 표준 규격에 맞게 입/출력을 제어하고, 시리얼 인터페이스 메모리 모듈에 기록, 삭제, 삭제 방지가 가능한 제어부를 포함을 특징으로 하는 USB 이동식 저장 장치.

#### 청구항 2

청구항 1에 있어서 시리얼 인터페이스 메모리 모듈은 상기 메모리 모듈을 구동하기 위한 전원선을 제외하고 데이터를 기록, 삭제, 삭제 방지를 위한 인터페이스 라인이 1개 이상 9개 이하의 신호선이 하나의 단위로 존재하여, 여기서 메모리 모듈이라 함은 상기 설정된 라인 단위 1개 혹은 2개 이상이 병렬로 구성 할 수 있다.

#### 청구항 3

청구항 2에 있어서 1개 혹은 2개 이상의 병렬로 존재하는 상기 메모리 모듈 군집이 또 다른 병렬 구조로 구성될 수 있고 상기 신호선의 단위로 1개 혹은 상기 메모리 군집의 병렬 개수 만큼 갖는 것을 포함한다.

#### 청구항 4

청구항 1에서 있어서 (c)항의 제어부는 적어도 하나이상의 시리얼 인터페이스 메모리에 FAT 파일 시스템을 구성하고, 상기 구성한 파일 시스템에 데이터를 기록, 변경 삭제가 가능하고, 상기 파일 시스템에 보안 토큰용 데이터에 대한 서명, 검증, 암호, 복호, 해쉬, 랜덤값 생성 및 기록, 변경, 삭제가 가능한 기능을 포함한다.

#### 청구항 5

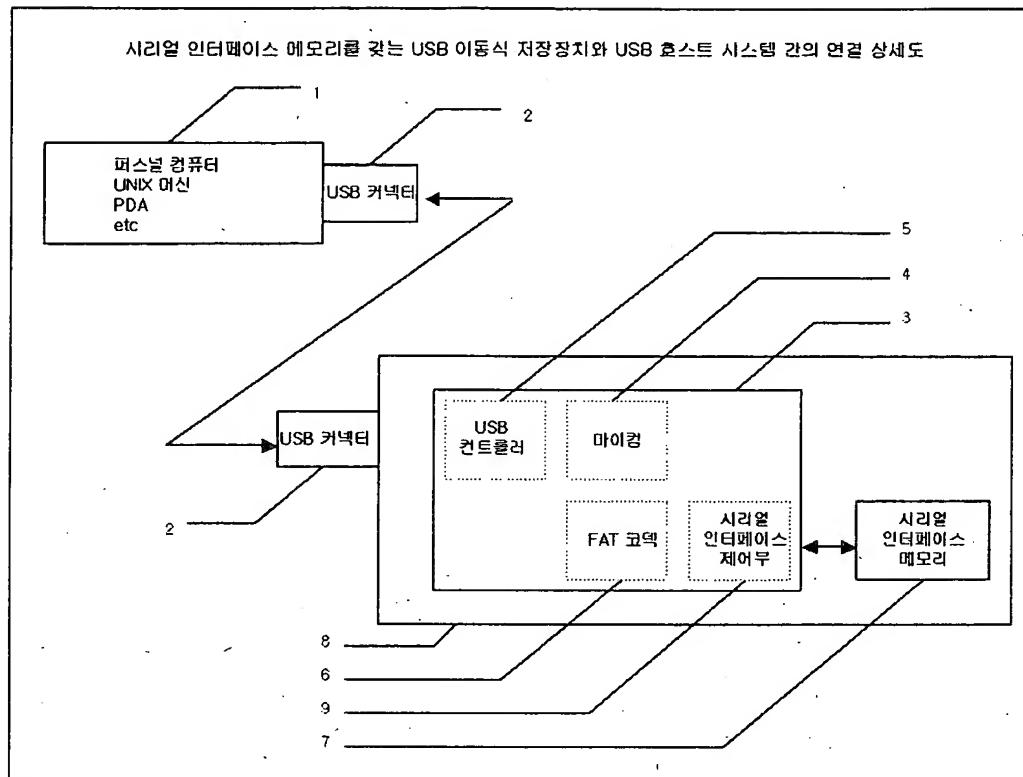
청구항 4에서 보안 토큰용 데이터를 다루기 위해 별도의 보안 토큰용 모듈 함수가 포함된 프로그램이나 전용 보안 토큰용 프로그램으로만 제어가 가능한 것을 특징으로 한다.

#### 청구항 6

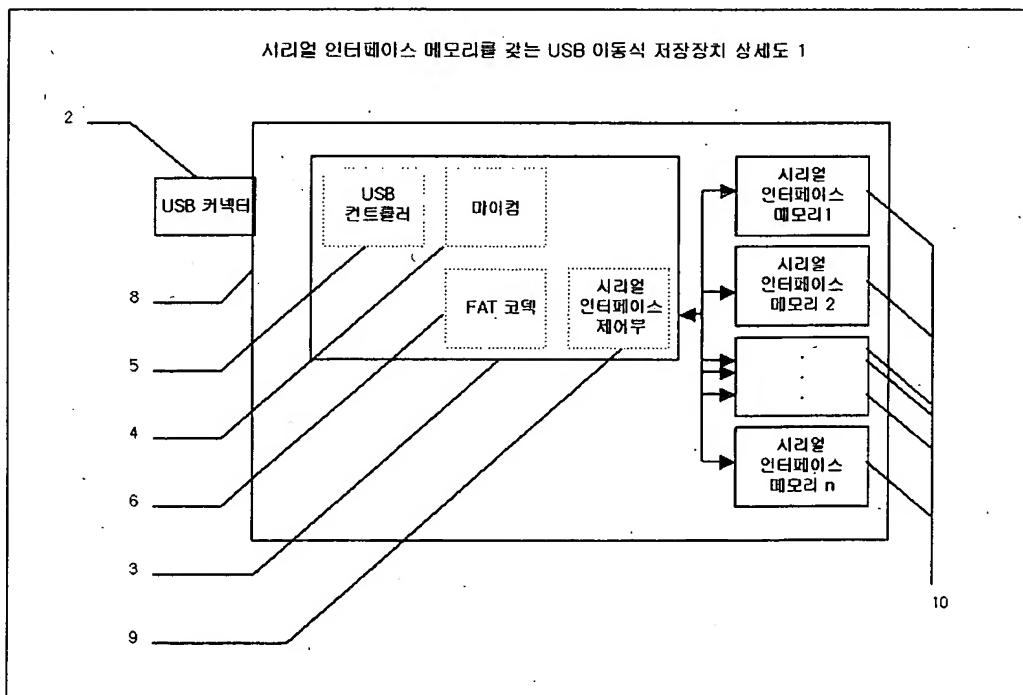
청구항 1에서 USB 커넥터는 USB 표준 버스 신호를 사용하는 변형된 모든 커넥터를 의미한다.

#### 도면

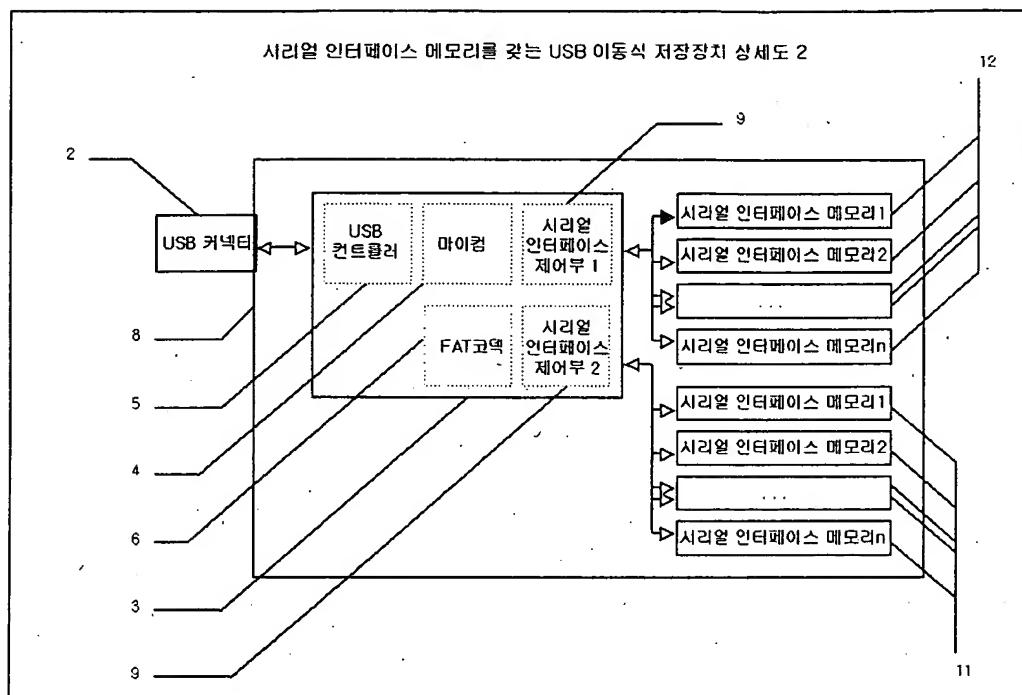
도면1



도면2



도면3



도면4

